ELSEVIER

Discrete Mathematics 208/209 (1999) 31–47

DISCRETE MATHEMATICS

Extended triple systems: geometric motivations and algebraic constructions

Lucien Beneteau

Institut National des Sciences Appliquées de Toulouse, Département Génie Mathématique, 31077 Toulouse Cedex, France

Received 5 March 1997; revised 21 May 1998; accepted 10 August 1998

Abstract

Extended triple systems (or ETSs for short) generalize the Steiner triple systems: they are provided with a collection of (unordered) triples $((x, y, z))$ in which multiple points are allowed. We still have the characterizing fact that any pair of points (x, y) lies in a unique $((x, y, z))$. This notion is thereby perfectly suitable for describing the situation of the cubic curves or cubic surfaces. The triples may be set under the form $(x, y, x \circ y)$ and then the mid-point binary law $x \circ y$ makes the set of points into a totally symmetric quasigroup. By choosing an origin u one gets some loop operation $x * y = u \circ (x \circ y)$. This algebraic approach is used so as to state structure theorems for special subcategories; for instance the entropic (or abelian) ETS, whose triples can be set under the form $(x, y, a - x - y)$ in the underlying set of some abelian group. By replacing the abelian group by some commutative Moufang loop in which the fixed element a is central with respect to the associativity, we obtain the wider category of the terentropic ETS. A 3-identity characterization of their related symmetric quasigroups is given. We call them Manin quasigroups. One may restate Manin's structure theorems in combinatorial terms as follows: in a suitable factor set of a cubic hypersurface the three-place relation of collinearity gives rise to an ETS which splits as a direct product $B \times H$ of a binary ETS B by some Hall triple system H. The difficult problem of finding eventually a cubic hypersurface whose related ETS is not entropic is not answered yet, as far as we know. But it may be reduced to the finding a surface whose related ETS is the famous 81-point triple system constructed by Marshall Hall Jr. We show that there exists exactly three non entropic Manin quasigroups of (minimum) order 81. Besides we present an exterior-algebra process that can be used for describing an important subcategory of Hall triple systems. © 1999 Elsevier Science B.V. All rights reserved.

Keywords: Steiner triple system; Cubic curve; Cubic surface; Symmetric quasigroup; Entropic quasigroup; Moufang loop; Hall triple system

E-mail address: beneteau@gmm.insa-tlse.fr. (L. Beneteau)

PII: S0012-365X(99)00060-6

1. Introduction

1.1. Convention

An unordered triple $((x,y,z))$ of elements from P is an equivalence class of (classical) triples (x,y,z): for any permutation x', y', z' of the three (not necessarily distinct) elements x, y, z, the triple (x',y',z') is another representative of $((x,y,z))$. The class of the triple (x,y,z) will be denoted by $((x,y,z))$ or simply $((xyz))$. The unordered triples are sometimes called 'lines' but we seldom use this terminology, for it could be confused here with other geometrical meanings.

Definition 1.1. An extended (or generalized) triple system (ETS) is a pair (P,T) where P is a set of elements — called the points of the system — and T is a given collection of 'unordered triples' of points with the property that any two (not necessarily distinct) points from P lie in exactly one triple of T.

1.2. Examples

Example 1 (*the 4-element space*). Let P be the 4-element set u,v,w,x, the triples being $((uuv))$, $((uuw)),((uux))$, $((vwx))$ and $((xxx))$, $((vvv))$, $((www))$.

Example 2. Binary triple system (a generalization): Let P be the underlying set of an elementary abelian 2-group, and let T be the collection of triples $((x,y,z))$ characterized by the relation $x+y+z=0$ (the identity element of the group).

Example 3. Affine triple system: Let P be the underlying set of some n-dimensional affine space $\mathrm{AG}(n,3)$ over the three-element field, and let T be the collection of triples $((xyz))$ whose three points either make up the 3 distinct points of an affine line, or satisfy $x=y=z$.

1.3. Comments about the notion of 'unordered triples'

There are 6 distinct representatives whenever x,y,z are pairwise distinct; the triple is then a 3-element line. But one has also 1-element lines $((xxx))$ with only one representative, and 2-element lines$((xxz))$ with 3 representatives when x and z are distinct; x is then called the double point of the 'tangent line' $((x,x,z))$. For instance, in a binary triple system, for any two distinct points x and y different from O, one has $2x+O=O=x+y+z$ with z different from x; so x is a double point of the line $((xxO))$ and at the same time a simple point in the line $((xyz))$.

1.4. Why 'extended' or 'generalized'? The best known case of the Steiner triple systems

There is absolutely no doubt that everybody's favorite examples of ETSs are the Steiner triple systems, up to a classical identification. In case a given ETS (P,L)

admits no 2-element lines, then any two distinct points lie in a unique 3-element line $((xyz)$. By defining the blocks as the related 3-element subsets x, y, z one gets then a $2-(v, 3, 1)$ design, namely a 'Steiner triple system'. Conversely, if (P, B) is a Steiner triple system whose set of blocks is B, by adding the collection of 1-element lines $((xxx))$ for any x from P, one recovers an ETS without 2-element lines.

One may thereby identify the Steiner triple systems with the ETSs without 2-element lines.

1.5. *The point-extension of the Steiner triple systems*

Another canonical way to obtain an ETS from a Steiner triple system (P, B) is to add a point o and to define the unordered triples $((xyz))$ as the equivalence classes of the triples (x, y, z) that are: either of the form (o, x, x) up to a permutation or such that $\{x, y, z\}$ is a block.

1.6. *Example*

The projective space $\mathrm{PG}(n, 2)$ over the 2-element field $\mathrm{GF}(2)$ may be considered as a Steiner triple system whose blocks are the projective lines. Its point-extension yields another description of the Binary triple system.

1.7. *Other generalizations of the Steiner triple systems*

There are other nice generalizations of the Steiner triple systems, for instance, the 'closed trail systems' discussed by Lindner and Rodger [11]: this time the triples are replaced by sequences of length $m > 2$ defined up to a cyclic shift. Subsequently, the term 'generalized triple systems' could be confusing. The usual terminology of ETSs is not much better, because such systems need not be constructible by an extension.

1.8. *The ETSs arising from collinearity in cubic curves and cubic hypersurfaces*

The notion of ETS is underlying in two works dealing respectively with cubic curves [7] and cubic hypersurfaces [12].

1.9. *Conventions*

In the n-dimensional projective space $\mathrm{PG}(n, K)$ over some field K, consider some absolutely irreducible cubic hypersurface S defined over K. Denote by $P = S_r(K)$ the set of regular (or non-singular) K-points of S.

Definition 1.2. The 'collinearity' is a three-place relation $\mathrm{Col}(x, y, z)$ defined in P: three not necessarily distinct points x, y, z are said to be collinear (abbreviated in $\mathrm{Col}(x, y, z)$)

when there exists a projective line L containing x, y, z such that one of the following two conditions holds:

(C1) x, y, z are the point-intersection of L with S, each point turning up equally often as its intersection multiplicity (usually denoted by the intersection cycle: $x + y + z = L.S$) or

(C2) L is completely contained in S.

The verification of the following statement is left to the reader:

Proposition 1.1. *The collinearity enjoys the following two properties*:

(i) '*total symmetry*': *if* $\mathrm{Col}(x, y, z)$ *holds, then* $\mathrm{Col}(x', y', z')$ *holds as well for any permutation* x', y', z' *of* x, y, z

(ii) '*never two without one third*': *for any two* (*not necessarily distinct*) *points* x, y *from* P, *there is at least one point* z *from* P *such that* $\mathrm{Col}(x, y, z)$ *holds.*

1.10. The ETS corresponding to cubic curves

Assume temporarily that S is a curve in $\mathrm{PG}(2, K)$. Since S is irreducible, the condition C2 is never obeyed, whence for any two (not necessarily distinct) points x, y from P, there is exactly one z from P such that $\mathrm{Col}(x, y, z)$ holds. Set $z = x \circ y$. Fix an element u from P and define another binary operation by

$$x *_u y = u \circ (x \circ y).$$

We have the following classical facts:

Proposition 1.2. *The set of unordered triples* $((xyz))$ *such that* $\mathrm{Col}(x, y, z)$ *holds endows the set* $P = S_r(K)$ *with a structure of ETS. Furthermore, the binary law* $x \circ y$ *satisfies the so-called* '*entropic identity*':

$$(x \circ y) \circ (z \circ t) = (x \circ z) \circ (y \circ t).$$

Theorem 1.3 (Lamé). *The operation* $x *_u y = u \circ (x \circ y)$ *endows the set* $P = S_r(K)$ *with a structure of abelian group.*

Definition 1.3. Any ETS (whether it arises from a cubic hypersurface or not) whose related law $x \circ y$ satisfies the entropic identity — or equivalently in which the binary law $x *_u y = u \circ (x \circ y)$ satisfies the associativity — is said to be 'entropic'.

1.11. Manin's ETS arising from a cubic hypersurface

In his attempt to generalize the theorem of Lamé to hypersurfaces of dimension > 1, Manin was led to a wider notion of ETS, which we call the 'terentropic ETSs'.

By convention they are characterized by the following condition:

(TE) any three points generate an entropic subsystem.

The terentropic ETSs that are Steiner triple systems are called 'Hall triple systems'.

We sketch Manin's main results. Observe that for a hypersurface S of dimension >1, the unicity of z from $P=S_r(K)$ such that $\mathrm{Col}(x,y,z)$ holds is no longer true for any two points x and y from P. Therefore Manin's structure of ETS related to $P=S_r(K)$ needs to be defined in a suitable factor-set $Q=P/R$ of $P=S_r(K)$ by some 'admissible relation' R (in the sense that if $\mathrm{Col}(x,y,z)$ and $\mathrm{Col}(x,y',z')$ hold then yRy' implies zRz'). One may state the following fact whose geometric justification is due to Bel'skii (see [12]).

Theorem 1.4. *In a Manin's ETS (Q,L) arising from a cubic hypersurface of dimension >1, each simple point t of a tangent triple $((xxt))$ is an inflexion point of (Q,L), namely $((ttt))$ is a triple.*

As a consequence one has the:

Theorem 1.5. *Any Manin's ETS (Q,L) arising from a cubic hypersurface of dimension 1 splits as a direct product $B.H$ of a binary ETS B by some Hall triple system H.*

1.12. Open question

The problem raised by Manin (see [12], II, Problem 11.11) of finding eventually a cubic hypersurface whose related ETS is not entropic concerns in fact the structure Hall triple system H appearing in the foregoing decomposition theorem. Is it always an affine ETS as it occurred in all the known examples? If it is not always the case, then there should exist a surface S and some admissible relation R in $P=S_r(K)$ such that the ETS defined in the factor-set $Q=P/R$ be the famous 81-point triple system constructed by Marshall Hall Jr [8]. We refer the reader to [12] chapters 1 and 2, and to [5], chapters 3 and 4, for a more detailed account of Manin's theory of cubic hypersurfaces.

1.13. The three points of view of the report

There are three aspects of ETSs we shall consider:

- the geometrical point of view yields motivations for studying some subcategories;
- the combinatorial point of view provide us with a descriptive terminology;
- lastly, the algebraic point of view that is to be detailed in the next section, because we need some efficient tools for studying terentropic ETSs. For various investigations concerning the ETSs, the best setting is loop theory where powerful results due to Bruck [4] can be used.

1.14. The classification results

We shall see that entropic ETSs are related to each abelian group. Though the correspondence is not one-to-one, the knowledge of the related abelian group determines the entropic ETSs up to isotopy. Recently Schwenk [14] obtained a classification of the finite entropic ETSs up to isomorphism. The classification of the finite terentropic ETSs up to isomorphism is much more difficult. They are related to some loops satisfying the square-distributivity, namely the identity: (SD) $x^2 * (y * z) = (x * y) * (x * z)$.

These loops are known to be the commutative Moufang loops (CMLs for short). There is a surjective correspondence from the category of the terentropic ETSs (P, L) (or Manin quasigroups $(P, .)$) onto the category of the commutative Moufang loops $(P, *) = ML((P, .))$. In this report we study particularly:

- the commutative Moufang loops with only one related terentropic ETS (or Manin quasigroup), up to isomorphism; and
- the commutative Moufang loops with exactly two related terentropic ETSs (or Manin quasigroups).

We present a useful characterisation for the first category, and a sufficient condition for belonging to the second one. Several applications are given. An exterior-algebra process is employed for constructing some Hall triple systems. Besides, we establish that there are exactly three nonentropic Manin quasigroups of (minimum) order 81; as an intermediary result we prove also that there are exactly two nonabelian commutative Moufang loops of (minimum) order 81.

2. The algebraic tools; characterization of the terentropic ETSs and Manin quasigroups

2.1. The mid-point law: the third point of the line

A natural way to define a first binary law in a given ETS (P, L) follows from the definition itself: for each pair (x, y) there is one and only one unordered triple of the form $((xyz))$, so one may set $z = x \circ y$. In view of the properties of the unordered triples it is clear that this law is totally symmetric in the sense that if $x \circ y = z$ holds then $x' \circ y' = z'$ holds as well for any permutation x', y', z' of x, y, z. Since $z = x \circ y$ is the third point of the line through x and y, and since this line contains three points (counting multiplicities), z can be viewed as the mid-point of x and y — though one has to keep in mind that in this context the mid-point can as well coincide with x (or y) even when x and y are different.

Definition 2.1. A quasigroup is a set $(Q, .)$ endowed with a binary operation $x.y$ such that, for any a and b from Q, the left multiplication $a.x$ and the right multiplication

$y.b$ are permutations of the set Q. If, moreover, there exists an identity element, one says that $(Q,.)$ is a loop.

Proposition 2.1. *In any set Q a binary operation $x.y$ is totally symmetric iff it is both multiplicatively involutive: ($x.(x.y)=y$ identically) and commutative. $(Q,.)$ is then a quasigroup that will be said to be totally symmetric.*

Proof. Straightforward verification. □

Theorem 2.2. *Any totally symmetric quasigroup $(Q,.)$ can be provided with a structure of ETS by deciding that the unordered triples are of the form $((xyz))$ with $x.y=z$. The so-defined correspondence between the totally symmetric quasigroups $(Q,.)$ and the ETSs (Q,L) is one-to-one.*

Proof. Left to the reader. □

Subsequently one identifies each totally symmetric quasigroup $(Q,.)$ with the so-constructed ETS (Q,L).

2.2. The loop-operation: the fourth point of the parallelogram

In what follows to any element u of a quasigroup $(Q,.)$ we attach the binary operation $x *_u y = u.(x.y)$. It is always a quasigroup operation. In case a quasigroup $(Q,.)$ is totally symmetric, the star-operation is furthermore commutative and admits u as an identity element: $(Q,*_u)$ is thus a commutative loop. Geometrically the resulting element $s = x *_u y$ is characterized by the equality of two mid-points: $u.s = x.y$, expressing that (u,x,s,y) is, so to speak, a parallelogram.

Theorem 2.3. *In a totally symmetric quasigroup $(Q,.)$, the four following conditions are equivalent:*

(i) *$(Q,.)$ is entropic;*
(ii) *$(Q,*_u)$ is entropic;*
(iii) *$(Q,*_u)$ is an abelian group for some u from Q;*
(iv) *$(Q,*_u)$ is an abelian group for any u from Q.*

When they are obeyed, up to isomorphism the abelian group $(Q,*_u)$ does not depend on the choice of the origin u in Q.

Proof. The direct verification is easy. Anyway these facts are subsumed by a further result (concerning the more general structure of the terentropic quasigroups) that is to be given an explicit proof here. □

Let us record that each entropic totally symmetric quasigroup $(Q,.)$ is related to an essentially unique abelian group $(Q,*_u)$.

Now any abelian group arises in this manner, since conversely one has the following canonical construction process for entropic totally symmetric quasigroup:

Proposition 2.4. *If $(A,+)$ is an abelian group, any binary law of the form $x.y=(c-x-y)$ makes A into an entropic totally symmetric quasigroup $(Q,.)$ such that the following equalities hold*:

$$x *_u y = u.(x.y) = x + y.$$

Proof. Straightforward calculation in the abelian group. □

Nevertheless one has to keep in mind that not-isomorphic entropic totally symmetric quasigroups may quite well be related to the same abelian group.

2.3. Example

If n is a multiple of 3 then in the cyclic group $(Z_n,+)$, the law $x \circ y=(1-x-y)$ admits no idempotent, while the law: $x.y=(-x-y)$ has O for idempotent. So $(Q,.)$ and (Q,o) are not isomorphic while their related group is $(Z_n,+)$.

2.4. The laws corresponding to the terentropic ETSs

We now turn to investigate the special category of the terentropic ETSs. They are identified with the terentropic totally symmetric quasigroups that we call the Manin quasigroups (they are called CH-quasigroups in Manins work, but it would not help much to adopt again this terminology here since the main remaining open question is to know whether some Manin quasigroups are actually constructible from cubic hypersurfaces).

We must first establish that square distributivity (SD):

$$x^2.(y.z)=(x.y).(x.z)$$

characterizes those totally symmetric quasigroups that are Manin quasigroups. Some preliminaries are needed.

Definition 2.2. In any CML $(Q,*)$ an element c is said to be associatively central if the associativity is satisfied with respect to any pair x,y of elements from Q, in the sence that: $(x*y)*c=x*(y*c)$ is satisfied. The set Z of all the associatively central elements is called the (associative) center of the CML $(Q,*)$-notation: $Z=Z(Q,*)$.

We shall need the following classical fact (see [1,4,5] for instance):

Theorem 2.5 (Moufang). *Any three elements x,y,c of a CML satisfying the associativity*: $(x*y)*c=x*(y*c)$ *span a subloop that is associative.*

2.5. Structure of the terentropic ETSs

Theorem 2.6. *Let (P, L) be any ETS with the mid-point law $x.y$* and the loop-operation $x *_u y = u.(x.y)$. *The five following conditions are equivalent*:

(i) *the ETS (P, L) (or the quasigroup $(P, .)$) is terentropic*;

(ii) *the mid-point law is square-distributive*;

(iii) *the mid-point law obeys the following identity*:

$$x.(y.z) = (x^2.y).(x.z);$$

(iv) *$(P, *_u)$ is a CML for some u from P*;

(v) *$(P, *_u)$ is a CML for any u from P.*

When they are fulfilled, up to isomorphism the CML $(P, *_u)$ does not depend on the choice of the 'origin' u. Besides $u^2 = u.u$ is associatively central in $(P, *_u)$, and the opposite of an element x with respect to the loop operation $(*_u)$ may be expressed by: $-_u x = u^2.x$. *One may recover the mid-point law from the star-operation by taking*

$$x.y = u^2 -_u (x *_u y).$$

Proof. It will be divided into three steps.

Step 1: Since the identity:

$$x^2.(y.z) = (x.y).(x.z)$$

may be viewed as a special case of the entropic law, (i) implies (ii). Now the mid-point law is totally symmetric, so the identity (SD) means that $a = (b.c)$ implies that $x^2.a = (x.b).(x.c)$. In other terms, $b = (a.c)$ implies that $(x.b) = (x^2.a).(x.c)$ again by total symmetry. But this last implication is just another way to express that the identity: $x.(y.z) = (x^2.y).(x.z)$ is fulfilled. Thus this identity is equivalent to (SD).

Step 2: We are by now in a position to establish that, if one assumes (SD), then any two loops $(P, *_u)$ and $(P, *_v)$ corresponding to different choices of the origin are always isomorphic. More precisely from the identities (SD) and (iii) it follows that the permutation of P defined by $f(z) = u.(v.z)$ satisfies:

$$\begin{aligned} f(x) *_v f(y) &= v.((u.vx).(u.vy)) = v.((u^2.(v^2.xy))) = (vu^2).(xy) \\ &= u.(v.(u.xy)) = f(x *_u y). \end{aligned}$$

In what follows the law $(x *_u y)$ is sometimes abbreviated in $(x * y)$. One checks easily that the fact that the mid-point law obeys the following identity:

$$x^2.(y.z) = (x.y).(x.z)$$

implies that (SD) holds as well for the loop-operation:

$$(x * x) * (y * z) = (x * y) * (x * z).$$

Whence $(P, *_u)$ is a CML. Moreover, $(x *_u y) *_u (u^2) = x *_u (y *_u (u^2))$, since:

$$u.((u.xy)u^2) = xy.((u^2.u^2.)) = u.(x.(u.yu^2)).$$

Therefore $u^2 = u.u$ is associatively central in $(P, *_u)$. Besides $-_u x = u^2.x$ follows from the foregoing verification:

$$(u^2.x) *_u x = u.((u^2.x).x) = u.(u^2) = u.$$

Lastly, $x.y = u^2 -_u (x *_u y)$ holds because:

$$u^2 -_u (x *_u y) = (u^2) *_u ((u^2.(uxy)) = u.(u^2(u^2.(uxy)) = x.y.$$

Step 3: It remains to be checked that, if one assumes that $(P, *_u)$ is a CML for any u from P, then the subquasigroup S of $(P, .)$ spanned by any three arbitrary elements x, y, u is entropic. As a consequence of various identities arising in Step 2, it turns out that the set S coincides with the subloop of $(P, *_u)$ spanned by x, y, u^2. Now in view of the identity:

$$(x *_u y) *_u (u^2) = x *_u (y *_u (u^2))$$

it then follows from the Moufang theorem that the subloop of $(P, *_u)$ spanned by x, y, u^2 is an abelian group. Therefore subquasigroup S of $(P, .)$ is entropic, which completes the proof. □

One may derive as an obvious consequence the following useful equational characterization for the Manin quasigroups:

Corollary 2.7. *The Manin quasigroups may be described as sets endowed with a commutative binary operation*: $x.y$ *such that* $x.(x.y) = y$ *and* $x^2.(y.z) = (x.y).(x.z)$ *identically*.

Definition 2.3. The CML $(P, *_u)$ is to be considered as the CML related to the Manin quasigroup $(P, .)$ (or to the terentropic ETS (P, L)). It is defined up to isomorphism. Notation: $(P, *_u) = \mathrm{ML}(P, .) = \mathrm{ML}(P, L)$.

3. Correspondence properties and classification results

3.1. ETSs and Manin quasigroups related to a given CML

In this section we fix some CML $(Q, *)$ and its associative center $Z = Z(Q, *)$. Define $T(Q, *)$ as the set all the 3-powers $(x * x * x)$.

Theorem 3.1. *For any* c *from* Z *the binary law*:

$$x \circ_c y = c - (x * y)$$

makes Q *into a Manin quasigroup* $\mathrm{MQ}(Q, *, c)$. *Besides if* $(Q, *) = (P, *_u) = \mathrm{ML}(P, .)$, *then by taking* $c = u^2$ *one recovers*: $x \circ_c y = x.y$.

Remark 3.1. The various Manin quasigroups related to $(Q, *)$ are isotopic, as Smith pointed out [16]. but they are not necessarily isomorphic as we have seen already in the special case of groups.

Proposition 3.2. *One may say that all the Manin quasigroups related to* $(Q, *)$ *are isomorphic iff any associatively central element of* $Z(Q, *)$ *is a* 3*-power* $(x * x * x)$ *or equivalently iff the associative center* $Z = Z(Q, *)$ *coincides with* $T(Q, *)$.

Proof. One knows that in any CML $Z(Q, *)$ contains $T(Q, *)$. Now if $c = (x * x * x)$, then $x \circ_c x = c - (x * x) = x$ and one checks that $\mathrm{MQ}(Q, *, c)$ is then isomorphic to the Manin quasigroup corresponding to the identity element O namely $\mathrm{MQ}(Q, *, O)$, whose binary law is $x \circ y = -(x * y)$. If $Z(Q, *)$ coincides with $T(Q, *)$, any Manin quasigroup related to $(Q, *)$ is isomorphic to $\mathrm{MQ}(Q, *, O)$, while if there exists a c in $(Z - T)$, the Manin quasigroup $\mathrm{MQ}(Q, *, c)$ does not admit idempotents, and may not be isomorphic to $\mathrm{MQ}(Q, *, O)$, so that there are at least two nonisomorphic Manin quasigroups related to $(Q, *)$. □

Corollary 3.3 (Schwenk [14]). *If* $(Q, *)$ *is a finite abelian group of order* n*, then all the Manin quasigroups related to* $(Q, *)$ *are isomorphic iff* n *if not divisible by* 3.

Proof. Here $Z = Z(Q, *)$ coincides with Q, and $t(x) = 3x$ is surjective onto Q iff $\mathrm{gcm}(n, 3) = 1$. □

Remark 3.2. Schwenk obtained also a nice classification theorem about the more general case any finite abelian group: if the decomposition of $(Q, *)$ as a direct product of cyclic prime power order subgroups involves k pairwise nonisomorphic factors of 3-power order, there are exactly $(k + 1)$ nonisomorphic Manin quasigroups related to $(Q, *)$ (see [15]).

3.2. Loops and Manin quasigroups related to a given Hall triple system

Recall that the Hall triple systems (HTSs for short) are defined as the terentropic any Steiner triple systems. We do not intend to give much details here about these systems whose properties have been extensively discussed in several papers. We refer the reader to [2,6,8,13,16] for more details.

Their related mid-point law is idempotent (as in any Steiner triple system). Since they are moreover terentropic, the square distributivity holds as well. So that the mid-point law is self-distributive too.

Theorem 3.4. *The HTSs are the ETSs whose related mid-point law is distributive, in the sense that the following identity holds*:

$$a \circ (x \circ y) = (a \circ x) \circ (a \circ y).$$

As for the loop operation, any nonvanishing element has order three: It is an exponent 3 commutative Moufang loop. Conversely, from any exponent 3 commutative Moufang loop one may recover a uniquely defined related HTS. This situation is thus much simpler than between the Manin quasigroups and the commutative Moufang loops, where the correspondence is only surjective a priori.

Theorem 3.5. *There are up to isomorphism one-to-one correspondences between three categories of structures*:

- *the Hall triple systems*;
- *the distributive Manin quasigroups*;
- *the exponent* 3 *commutative Moufang loops.*

3.3. The kinship between HTSs and exponent 3 commutative Moufang loops

It recalls the kinship between affine spaces and vector spaces. The classification theorems concerning the HTSs had been derived from their algebraic description in quasigroup theory, either in terms of distributive Manin quasigroups or in terms of exponent 3 commutative Moufang loop. Exterior algebra was used also to provide explicit descriptions of these systems.

3.4. Example

Let $H(n)$ be some $(n+1)$-dimensional vector space over GF(3), with $n>2$. Pick up some basis: $e_0e_1e_2\ldots e_ie_{n-1}e_n$. For any two points: $x=\sum_i a_ie_i$ and $y=\sum_i b_ie_i$ let us set $z=x\circ y$ defined by

$$z=(a_1-b_1)(a_2b_3-a_3b_2)e_0-x-y.$$

This defines a totally symmetric operation on $H(n)$. One has either $x=y=z$ or the 3 points x,y,z are pairwise dictinct. The 3-subsets of the form x,y,z such that $z=x\circ y$ provide $H(n)$ with a structure of HTS will be refered to as $H(n)$ in what follows.

Theorem 3.6. *Any HTS has for cardinal number a* 3*-power* 3^m. *Nonaffine order* 3^m *HTSs exist for any* $m>3$. *For the order* 3^4 (*resp.* 3^5) *there is only one nonaffine HTS*, *namely* $H(3)$ (*resp.* $H(4)$).

Note that the existence of nonaffine HTSs of order $3^m>3^3$ is provided by $H(m-1)$. All the HTSs of order at most 3^7 have been classified by now (Table 1).

Definition 3.1. The rank r of an HTS is the smallest integer r such that there exists a generator set of r points.

Table 1
Maximum number of nonisomorphic HTSs of order 3^m

	Order							
	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8
Affine HTS	1	1	1	1	1	1	1	1
Nonaffine HTS	0	0	0	1	1	3	12	>41

Table 2
Number of nonisomorphic HTSs of order 3^m of rank p

	Order				
	3^4	3^5	3^6	3^7	3^8
Rank 4 HTSs	1	0	0	0	0
Rank 5 HTSs	1	1	1	1	4
Rank 6 HTSs	0	1	2	6	>15
Rank 7 HTSs	0	0	1	5	??
Rank 8 HTSs	0	0	0	1	??
Rank 9 HTSs	0	0	0	0	1

Theorem 3.7. *In any order 3^m HTS the rank r is at most $m+1$, with equality only in the entropic (or affine) case. Each minimal generator subset contains r points.*

The notion of rank allows us to state further classification facts (Table 2).

3.5. Construction of some HTSs via exterior algebra

The example of $H(n)$ may be generalized as follows. Consider some $(n+1)$-dimensional vector space S over GF(3), with $n>2$, and a chosen basis: $e_o e_1 e_2 \dots e_i$ $e_{n-1} e_n$ of S. For any two points: $x=\sum_i a_i e_i$ and $y=\sum_i b_i e_i$ let us set $z=x\circ y$ determined by

$$x+y+z=\left(\sum_{ijk,i<j<k} l_{ijk}(a_i-b_i)(a_j b_k-a_k b_j)\right)e_o,$$

where $(l_{ijk})_{i<j<k}$ is a nonvanishing sequence of elements from GF(3). This defines a binary operation of distributive Steiner quasigroup on S. The corresponding HTS has rank $n+1$.

Theorem 3.8. *Any rank $(n+1)$ HTS of order 3^{n+1} arises in this way.*

Let $V=V(n+1,\mathrm{GF}(3))$ be the n-dimensional vector space over GF(3) spanned by $e_o e_1 e_2 \dots e_i e_{n-1} e_n$.

Consider again a nonvanishing sequence:

$$(l_{ijk})_{i<j<k}$$

of elements from GF(3). The equalities:

$$g(e_i, e_j, e_k) = l_{ijk}$$

for $i<j<k$ define a unique symplectic trilinear form g from V^3 onto GF(3). Any two symplectic trilinear forms g and g' are said to be equivalent when $g'(x,y,z) = g(f(x), f(y), f(z))$ for some automorphism f of V. One shows that two sequences (l'_{ijk}) and (l_{ijk}) give rise to equivalent symplectic trilinear forms iff their related HTSs are isomorphic. The so-defined correspondence between rank $n+1$ HTSs of order 3^{n+1} and nonvanishing symplectic trilinear forms of $V = V(n, \mathrm{GF}(3))$ is one-to-one up to isomorphism for HTSs and up to equivalence for symplectic trilinear forms.

Furthermore this correspondence may be extended. Let $V = V(n, \mathrm{GF}(3))$ and $W = V(m, \mathrm{GF}(3))$ be vector spaces over GF(3) of dimension n and m, respectively. The set $\mathrm{AT}(n,m)$ of symplectic trilinear mappings from V^3 to W whose images have rank m may be provided with a natural notion of equivalence (up to compositions with linear isomorphisms of V and W). Let us denote by $a(n,m)$ the number of equivalence classes. Some process of construction shows that any class is related to an essentially unique HTS (see [2]). One may derive

Theorem 3.9. *If $m = 1, 2$ or 3, then $a(n,m)$ coincides with the maximum number $s(n,m)$ of pairwise nonisomorphic rank $n+1$ HTSs of order 3^{n+m}. If $m \geqslant 4$, then $s(n,m) \geqslant 3 + a(n,m)$.*

3.6. The terentropic ETSs that are nonentropic of smallest order

The aim of this section is to establish the following main statement:

Theorem 3.10. *There are up to isomorphism exactly three nonentropic Manin quasigroups of* (*minimum*) *order* 81.

We must first determine the nonabelian commutative Moufang loops of order 81. It turns out that there are exactly two such loops.

Lemma 3.11. *Any nonabelian exponent* 3 *CML $(Q,*)$ is related to two Manin quasigroups at least. When its center $Z = Z(Q,*)$ has minimum order* 3, *then $(Q,*)$ is related to exactly two Manin quasigroups.*

Proof. $T(Q,*)$ is reduced to the identity element O. Now if c is an arbitrary element from $Z\ O$, we have a Manin quasigroup $\mathrm{MQ}(Q,*,c)$ that is not isomorphic to $\mathrm{MQ}(Q,*,O)$. Besides one checks that $\mathrm{MQ}(Q,*,c)$ is isomorphic to $\mathrm{MQ}(Q,*,-c)$. Thus if $(Z-O)$ consists of just the two elements c and $-c$, one has only two related Manin quasigroups namely $\mathrm{MQ}(Q,*,c)$ and $\mathrm{MQ}(Q,*,O)$. □

Theorem 3.12. *For $n=3$ and for any $n\geqslant 5$ there exists at least one rank n exponent 3 CML of order 3^{n+1} which is related to exactly two Manin quasigroups.*

Proof. For $n>4$, an explicit exterior-algebra construction may be provided. One has to make choice of $z=x\circ y$ determined by

$$x+y+z=\left(\sum_{ijk,i<j<k} l_{ijk}(a_i-b_i)(a_jb_k-a_kb_j)\right)e_o,$$

where $(l_{ijk})_{i<j<k}$ is a sequence of elements from GF(3) such that any $i=1,2,\ldots,n$ occurs in exactly one 3-set i,j,k whose corresponding coefficient l_{ijk} does not vanish. Note that this does not hold for $n=4$ since there is no such sequence $(l_{ijk})_{i<j<k}$ in this case: there is no way to cover up the 4-set $S=1,2,3,4$ by some 3-subsets such that any element from S belongs to exactly one 3-subset. For $n=3$ one may in fact prove the unicity: there exists just one rank 3 exponent 3 CML, say $(H(3),*)$ of order 3^4 which is related to exactly two Manin quasigroups. As a set, $H(3)$ is described by taking $n=3$ in the previous example and its loop binary law is defined as

$$x*y=x+y-(a_1-b_1)(a_2b_3-a_3b_2)e_o.$$

This defines an exponent 3 CML operation. The two related Manin quasigroups $(H(3),o)$ and $(H(3),.)$ arise if one defines $x\circ y$ as in the previous example and $x.y$ by

$$x.y=-x-y+e_o+(a_1-b_1)(a_2b_3-a_3b_2)e_o.$$

This completes the proof. □

Lemma 3.13. *The CML $(K,*)$ generated by two elements u, v and w submitted to the three following relations*:

$$u^3=1=v^3 \quad \textit{and} \quad (u*v)*w=u*(v*w)*w^3$$

is of order 81.

Proof. One may readily check that any element from K may be written under the form: $X=u^a*v^b*w^c$ where a,b are integers modulo 3 and c is an integer modulo 9. The product of any two such elements $X=u^a*v^b*w^c$ and $X'=u^d*v^e*w^f$ is given by $X*X'=u^h*v^i*w^j$ where $h=a+d$; $i=b+e$ and $j=c+f+3(d-a)(bf-ce)$.

Conversely a straightforward verification shows that the direct product $Z_3.Z_3.Z_9$ organized with the binary law:

$$(a,b,c)*(d,e,f)=(h,i,j)$$

defined by the foregoing equalities is an exponent 9 CML spanned by the three triples $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$ that obey the two required relations

$$u^3=1=v^3 \quad \text{and} \quad (u*v)*w=u*(v*w)*w^3,$$

which completes the proof. □

Theorem 3.14. *Any nonassociative CML has for order a multiple of* 81, *and the CMLs* $(K, *)$ *and* $((H(3),_*)$ *are the only order* 81 *nonassociative CMLs.*

Proof. Let $(G, *)$ be some arbitrary nonassociative finite CML of order n. It is well known that G splits as a direct product $A.H$ of an abelian group A of order prime to 3 and a 3-power order CML H. In view of the Moufang theorem, H may not be generated by only two elements so that the index of its Frattini subloop $\mathrm{Fr}(H)$ is at least 3^3. Now $\mathrm{Fr}(H)$ contains the derived subloop whose order is at least 3. Hence n is divisible by $d = 3[H\colon\ \mathrm{Fr}(H)]$. Now d is a 3-power which is at least: $3^4 = 81$.

Assume now that $n = 81$. Necessarily $n = d$, $G = H$, and $[G\colon\ \mathrm{Fr}(G)] = 3^3$. Besides $\mathrm{Fr}(G) = D(G)$, and $D(G)$ is of order 3. If G has exponent 3 then G is the free loop $(H(3), *)$.

From now on, let us assume on the countrary that G is not of exponent 3. Since $T(G)$ is a nontrivial subloop of $\mathrm{Fr}(G) = D(G)$, one has $T(G) = \mathrm{Fr}(G)$. The endomorphism $h(x) = x^3$ has a kernel N that is a maximal subloop. Hence N contains $\mathrm{Fr}(G)$. Now $[G : \mathrm{Fr}(G)] = 27$ so $[N : \mathrm{Fr}(G)] = 9$ and one may take two elements u and v from N such that the factor loop $N/\mathrm{Fr}(G)$ is generated by the cosets of u and v modulo $\mathrm{Fr}(G)$. If w is any element from $(G - N)$ then G is spanned by u, v, w.

Moreover, both elements w^3 and $(u * (v * w))^{-1} * ((u * v) * w)$ are generators of the order 3 group $D(G)$, so that either

$$(u * (v * w))^{-1} * ((u * v) * w) = w^3$$

or

$$(u * (v * w)) * ((u * v) * w)^{-1} = w^3.$$

In the second case, by replacing u by u^{-1} one gets back to the situation of the first equality. Since u and v belong to N, one has also $u^3 = 1 = v^3$ so that G is isomorphic to K. This completes the proof. □

Theorem 3.15. *There are only three nonentropic Manin quasigroups of order* 81: *the quasigroups* $(H(3), o)$ *and* $(H(3), .)$, *and the Manin quasigroup* (K, o) *whose binary law is defined by* $x \circ y = -x - y$ *in the loop* $(K, *)$.

Proof. Any Manin quasigroup of order 81 is related to one of the two CMLs of order 81. If the related CML has exponent 3 then its center is a 3-order group and there are only two possibilities, namely $(H(3), o)$ and $(H(3), .)$. If the related CML has exponent 9 then it is $(K, *)$ whose center coincides with $T(K)$; whence it must be the quasigroup (K, o) described in the statement. This completes the proof. □

4. For further reading

The following references are also of interest to the reader: [3], [9] and [10].

References

[1] L. Bénéteau, Free commutative Moufang loops and anticommutative graded rings, J. Algebra 67 (1980) 1–35; MR 82 c 118.
[2] L. Bénéteau, J. Lacaze, Symplectic trilinear forms, related designs and quasigroups, Comm. Algebra 16 (5) (1988) 1035–1051.
[3] F.E. Bennett, N.S. Mendelsohn, On the existence of extended triple systems, Utilitas Math. 14 (1978) 249–267.
[4] R.H. Bruck, A Survey of Binary Systems, Springer, Berlin, 1958; M R 20, 76.
[5] O. Chein, H.O. Pflugfelder, J.D.H. Smith, Quasigroups and Loops; Theory and Applications, Sigma Series in Pure Mathematics, vol. 8, Heldermann, Berlin, 1990.
[6] C.J. Colburn, J.H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, 1996.
[7] I.M.H. Etherington, Quasigroups and cubic curves, Proc. Edinburgh Math. Soc. 14 (2) (1964/65) 273–291.
[8] M. Hall Jr., Automorphism of Steiner triple systems, IBM J. Res. Dev. (1960) 406–472.
[9] D.M. Johnson, N.S. Mendelsohn, Extended triple systems, Aequationes Math. (3) (1972) 291–298.
[10] T. Kepka, Structure of triabelian quasigroups, Comment Math. Univ. Carolinae 17 (1976).
[11] C. Lindner, C.A. Roger, The complete solution of the problem of equationally defining closed trail systems of K13, Bull ICA 11 (1994) 84–95.
[12] Yu.I. Manin, Cubic Forms, North-Holland, Amsterdam, London, 1974.
[13] G. Razafimanantsoa, La k-nilpotence minimale dans les boucles de Moufang commutatives; classification partielle des applications trilinéaires alternées, Thèse, Univ. Toulouse III, 1988, no. 3511.
[14] J. Schwenk, A classification of abelian quasigroups, Rend. Math. Appl. (7) 15 (2) (1995) 161–172.
[15] J.D.H. Smith, Finite equationally complete entropic quasigroups, Contribution to general algebra, Proc. Klagenfurt Conf., 1978, pp. 345–355.
[16] H.P. Young, Affine triple systems and matroid designs, Math. Z. 132 (1973) 343–359.